AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Texas

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

The SUBJECT PREMISES located at 751 Hebron Park Way, Suite 110, Lewisville, Denton County, Texas, 75057 as more fully described in Attachment A

Case No. 4:19MJ552

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

The SUBJECT PREMISES located at 751 Hebron Park Way, Suite 110, Lewisville, Denton County, Texas, 75057, as more fully described and depicted in Attachment A, which is attached hereto and incorporated herein by reference.

located in the Eastern District of Texas, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is attached hereto and incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC § 371 & 42 USC § 1320a-7b -	Conspiracy to Defraud the US & to Pay/Receive Health Care Kickbacks;
18 U.S.C.§ 1343 -	Wire Fraud;
18 U.S.C.§ 1347 -	Health Care Fraud; and
18 U.S.C. § 1349 -	Conspiracy to Commit Health Care Fraud

The application is based on these facts:

See Attached Affidavit of SA Jason T. Seth, United States Department of Health and Human Services, Office of the Inspector General, which is attached hereto and incorporated herein by reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SA Jason T. Seth, HHS-OIG
Printed name and title

Sworn to before me and signed in my presence.

Date: 09/25/2019 5:38pm

Judge's signature

City and state: Sherman, Texas

Hon. Christine A. Nowak, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Jason T. Seth, being duly sworn, depose and state under oath the following:

I. INTRODUCTION

1. I make this affidavit in support of an application pursuant to Federal Rule of Criminal Procedure 41 for a warrant to:

a. search the offices of Trinity Clinical Laboratories, LLC ("Trinity Labs") 751 Hebron Park Way, Suite 110, Lewisville, Texas, 75057 (the "**Target Location**") and more fully described in Attachment A, and to seize the items described in the following paragraphs and in Attachment B.

II. AGENT BACKGROUND

2. I am a Special Agent with the United States Department of Health and Human Services, Office of the Inspector General ("HHS-OIG") and have held this position since July 2018. As a Special Agent, my duties include, in part, investigating allegations of health care fraud affecting public health care benefit programs, such as Medicare and Medicaid. Prior to my employment with HHS-OIG, I was a Special Agent with the The United States Army, Criminal Investigation Division Command, from 2013 until 2016. I graduated with a Master's degree in Digital Forensic and Cyber Investigations and a Bachelor's degree in Accountig with a minor in Business Administration from University of Maryland, Adelphi, Maryland. I graduated from the Federal Law Enforcement Training Center in 2018, where I received training in how to conduct complex criminal investigations and how to comply with federal search and seizure procedures. I received specialized training in the Health Care Fraud Investigations Training Program, Digital Forensic and Cyber Investigations Training Program, Child Abuse Prevention and Investigative

Techniques Training Program, Advanced Crime Scene Investigation Techniques Training Program, and Special Victim Unit Investigator Course.

3. I have participated in complex interstate criminal investigations with special agents and investigators from other federal and state law enforcement agencies. I have participated in the execution of multiple search warrants resulting in the seizure of evidence relating to criminal activity. I have reviewed numerous forms of evidence, including Medicare and Medicaid claims data, medical records, and other business records. During my training, education and experience, I have become familiar with white-collar fraud schemes, including schemes involving public health care benefit programs. I am familiar with business practices used by individuals in the health care industry, including documents used in and maintained by health care providers in the administration of medicine as well as in the ordinary course of business.

4. This affidavit is submitted in support of the Government's application for a search warrant of the **Target Location**. Based on my training and experience, the facts as set forth in this affidavit, and the investigation to date, I submit that there is probable cause to believe there are documents and items that are evidence of a crime, fruits of a crime, or other items illegally possessed or property designed for use, intended for use or used in a crime, in violation of 18 U.S.C. § 371 (Conspiracy to Defraud the United States and to Pay and Receive Health Care Kickbacks), 42 U.S.C. § 1320a-7b (Anti-Kickback Statute), 18 U.S.C.§ 1343 (Wire Fraud); 18 U.S.C.§ 1347 (Health Care Fraud), 18 U.S.C. § 1349 (Conspiracy to Commit Health Care Fraud), and (collectively, the "**Target Offenses**") within the **Target Location** and committed by persons known and unknown, including but not limited to John Grisham and Lori Grisham, who are married and co-owners of Trinity Labs along with other individuals and businesses, known and unknown, in this investigation.

5. I further submit that based on the evidence set forth below, and all reasonable inferences from that evidence, there is probable cause to believe that evidence, instrumentalities, and fruits of these violations, as more fully described in Attachment B, will be found on or in the property identified and described in Attachment A, *i.e.*, the **Target Location**.

6. I base this affidavit on my investigation, information provided to me by other law enforcement agents, public sources and business records, and my experience as a Special Agent. Because I submit this affidavit for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation. Where I set forth the statements of others in this affidavit, I set forth in substance and in part.

III. THE MEDICARE PROGRAM

7. The Medicare program ("Medicare"), established under Title XVIII of the Social Security Act, is a federal health care program the provides benefits to persons who are sixty-five years of age or older or disabled. Medicare is administered by the Centers for Medicare and Medicaid Services ("CMS"), a federal agency under the United States Department of Health and Human Services. Individuals who receive benefits under Medicare are referred to as Medicare "beneficiaries." Medicare is a health care benefit program as defined by 18 U.S.C. § 24(b).

8. Medicare has four parts: hospital insurance (Part A), medical insurance (Part B), Medicare Advantage (Part C), and prescription drug benefits (Part D).

9. Medicare Part A Hospital Insurance ("Medicare Part A") helps cover medically necessary inpatient care services in hospitals, including critical access hospitals, and skilled nursing facilities. It also covers hospice care and some home health care.

10. Medicare Part B Medical Insurance ("Medicare Part B") helps cover doctors'

services and outpatient care. It also covers some of the services of physical and occupational therapy, and some home health care. Medicare Part B helps pay for these covered services and supplies when they are medically necessary.

11. Under the Medicare Prescription Drug, Improvement, and Modernization Act of 2003, Medicare Part C, also known as the "Medicare Advantage" Program, authorizes CMS to contract with public or private organizations to offer a variety of health plan options for beneficiaries, including coordinated care plans (such as health maintenance organizations, provider sponsored associations, and preferred provider organizations), Medicare Medical Savings Account plans, and private-fee-for-service plans. Medicare Advantage provides beneficiaries with all of the same services provided by original fee-for-service Medicare plan, in addition to mandatory supplemental benefits and optional supplemental benefits.

12. "Providers" are laboratories, physicians, and other health care entities who provide services to Medicare beneficiaries. Medicare providers are required to submit an application, in which they agree to comply with all Medicare-related laws and regulations. A Medicare "provider number" is assigned to a provider upon approval of the provider's Medicare application. A provider can use that provider number to file claims with Medicare to obtain reimbursement for services rendered to beneficiaries. Medicare publishes guidance regarding what services it will and will not pay for in a variety of publications, including by issuing National Coverage Determinations.

A. Genetic Screening Tests

13. Cancer Genetic Testing ("CGx") is a type of genetic test administered for patients with a genetic predisposition to cancer. Medicare issued National Coverage Determination 90.2, effective March 16, 2018, which states: "Patients with cancer can have

recurrent, relapsed, refractory, metastatic, and/or advanced stages III or IV of cancer. Clinical studies show that genetic variations in a patient's cancer can, in concert with clinical factors, predict how each individual respond to specific treatments." Accordingly, Medicare will reimburse genetic screening tests for beneficiaries with a diagnosis of cancer when ordered by a treating physician for the purpose of determining the proper course of treatment for the beneficiary.

14. Title XVIII of the Social Security Act (SSA) § 1862(a)(1)(A), states that no Medicare payment shall be made for items or services that "are not reasonable and necessary for the diagnosis or treatment of illness or injury or to improve the functioning of malformed body member." Title 42, Code of Federal Regulations § 410.32 provides:

> a. All diagnostic x-ray tests, diagnostic laboratory tests, and other diagnostic tests must be ordered by the physician who is treating the beneficiary, that is, the physician who furnishes a consultation or treats a beneficiary for a specific medical problem and who uses the result in the management of the beneficiary's specific medical problem. Tests not ordered by the physician who is treating the beneficiary are not reasonable and necessary.

15. Accordingly, Medicare does not reimburse for genetic screening tests performed simply to determine the likelihood a beneficiary will or will not develop cancer in the future. Rather, Medicare will pay only for genetic screening tests performed to aid in the treatment of a beneficiary with a personal diagnosis of cancer. Medicare reimburses for the test at rates varying from approximately a few hundred dollars to over $6,000 for a panel of tests.

IV. BACKGROUND OF ENTITIES AND INDIVIDUALS

16. Trinity Labs is a Medicare provider with a principal place of business at the Target Location that purports to provide genetic screening tests to Medicare beneficiaries. Between in or

around April 2018 through in or around June 2019, Trinity Labs submitted approximately $89.2 million for genetic screening tests, of which Medicare paid approximately $35.3 million.

17. MedSymphony, LLC ("MedSymphony") is a company with its principal place of business at 53 North Calibogue Cay Road, Hilton Head Island, South Carolina, 29928, located in Beaufort County, South Carolina. Meetmydoc LLC ("Meetmydoc") is a company with its principal place of business at 53 North Calibogue Cay Road, Hilton Head Island, South Carolina, 29928, located in Beaufort County, South Carolina. MedSymphony and Meetmydoc, hereinafter referred to collectively as the "MedSymphony Entities," purportedly provide telemedicine services to Medicare providers and beneficiaries.

18. John Berberian ("Berberian"), a resident of Atlanta, Georgia is the owner of consulting companies, including HSD Management, LLC, HSD Consultants LLC, and HSD Financial, LLC. Through these companies, investigators have learned that Berberian purportedly provides consulting services to Medicare providers, such as Trinity Labs.

19. PerkinElmer Genomics ("PerkinElmer") is a company incorporated under laws of Pennsylvania with its principal place of business at 250 Industry Drive, Suite 400, Pittsburg, PA 15275. PerkinElmer is a corporation focused in the business areas involving biochemical, metabolic and genetic screening tests.

20. Scott Global, LLC ("Scott Global") is a company incorporated under the laws of Florida with its principal place of business at 14 East Washington Street, Suite 406, Orlando, Florida, 32801, located in Orange County, Florida. Ivan Scott, a resident of Osceola County, Florida, is the owner of Scott Global. Tiffany Scott, a resident of Osceola County, Florida, is Ivan Scott's spouse and an associate at Scott Global. Scott Global is a purported marketing services company that provides marketing services to Medicare providers.

21. Company 1 is a company incorporated under the laws of Florida with a principle place of business located in Broward County, Florida. Company 1 is a purported marketing and recruiting company with call centers located in Florida. Confidential Human Source 1 (the "CHS 1"), a resident of Broward County, Florida, is a co-owner of Company 1, Confidential Human Source 2 (the "CHS 2"), a resident of Broward County, Florida, is a co-owner of Company 1.

V. PROBABLE CAUSE REGARDING THE TARGET OFFENSES

22. Probable cause regarding the specified **Target Offenses** is established by statements from CHS 1 and CHS 2, electronic communications, public records, Medicare records including claims data, and financial records.

23. I know from my training and experience that certain Medicare providers that conduct genetic screening tests engage in fraud by pushing genetic screening test kits and related materials on Medicare beneficiaries who do not have a medical need for these items.

24. I also know from my training and experience that such Medicare providers often use call centers to market genetic testing kits aggressively to Medicare beneficiaries, without regard to whether the tests are medically necessary. Based on my training and experience, I also know that these call centers often contract with telemedicine companies who provide doctors to perform "telemedicine" consultations with Medicare beneficiaries to justify the issuance of a doctor's order for these items. Based on my training and experience, I know that in some cases, these doctors do not actually perform the telemedicine consultation with the beneficiaries, and, in exchange for an illegal kickback and bribe, instead authorize the tests without conducting valid examinations of the beneficiaries.

25. To date, this investigation has revealed that Trinity Labs has paid illegal kickbacks and bribes to Company 1. In turn Company 1 has paid illegal kickbacks and bribes to telemedicine

companies, such as MedSymphony, all in exchange for the referral of Medicare beneficiaries that Company 1 provided to Trinity Labs for genetic screening tests that are medically unnecessary, not eligible for Medicare reimbursement, and/or not provided as represented.

26. Moreover, to date, this investigation has revealed that the genetic screening tests submitted by Trinity Labs or caused to be submitted by Trinity Labs to Medicare for payment or reimbursement are *per se* medically unnecessary under Medicare rules and regulations since no medical professionals were identifying and determining whether a beneficiary should complete a genetic screening test before a doctor got involved in the process.

A. Summary of the Investigation and the Fraudulent Scheme

(i) Trinity Labs

27. Trinity Labs submitted and caused the submission of Medicare claims for genetic screening tests of Medicare beneficiaries, purportedly to determine predisposition to various types of cancer. In order to submit claims to Medicare, Trinity Labs needed (a) eligible Medicare beneficiaries who received the genetic screening test kits, and (b) prescriptions issued by doctors for the genetic screening tests, also known as doctor's orders ("DOs").

28. During the course of this investigation, law enforcement agents have learned that Trinity Labs paid Company 1 illegal kickbacks and bribes to obtain the required personal identification information for eligible Medicare beneficiaries and DOs. In turn, Company 1 obtained the Medicare beneficiaries' identification information who received the genetic screening tests and DOs by paying illegal kickbacks and bribes to Scott Global. Company 1 collaborated with Scott Global and other purported marketers, who obtained the beneficiaries by running a call center located in Florida that aggressively marketed genetic screening test services and obtained DOs by paying illegal kickbacks and bribes to MedSymphony, a telemedicine company.

29. Between May 2019 and August 2019, CHS 1 and CHS 2 were interviewed by law enforcement agents on several occasions. During the interviews, CHS 1 and CHS 2 stated that they were introduced to Trinity Labs by Berberian. Company 1 first conducted business with Trinity Labs through one Berberian's companies named Hospital Service Direct ("HSD").

30. Bank records, obtained through grand jury subpoenas, confirm that Trinity Labs sent an interstate wire of approximately $3 million to HSD from on or about May 6, 2019 to on or about May 20, 2019 from a Wells Fargo Bank account ending with 6339.

31. CHS 1 and CHS 2 also explained that Company 1 had a business agreement with Trinity Labs wherein Company 1 identified and shipped genetic testing kits to beneficiaries.[1] Upon confirmation of delivery, Company 1 employees would call the beneficiaries with step-by-step instructions for the swabbing test. The beneficiaries would then mail the completed swab back to Company 1.

32. After receiving the completed swab from the beneficiaries, Company 1 employees called the beneficiaries once again and interviewed him or her to obtain at least three symptom codes, in an effort to justify the medical necessity of the genetic test. Company 1 employees making these calls did not have medical licenses or training, nor were they under the supervision of anyone with a medical license.

33. Company 1 contracted with MedSymphony to obtain DOs for the genetic tests. CHS 1 and CHS 2 explained that MedSymphony completed DOs for Company 1. Company 1 uploaded recorded symptom code phone calls with beneficiaries, as well as forms Company 1 completed in connection with the call to the beneficiaries, onto a portal controlled by

[1] DNA samples were collected from beneficiaries primarily through a "buccal swab," which is a manner of collecting DNA from the inside of a person's cheek using sterile swabs with cotton tips.

MedSymphony. MedSymphony then sent alerts to doctors about orders pending their approval.

34. Additionally, CHS 1 stated that after Company 1 obtained the DO from MedSymphony, Company 1 then packaged the completed swab and DO for shipment to Trinity Labs. Then Trinity Labs billed Medicare for conducting genetic testing on the completed swab and used a portion of the money paid by Medicare to compensate Company 1 for the completed swab and DO.

35. During interviews, CHS 1 and CHS 2 stated that Trinity Labs paid Company 1 for their services through Berberian' s company, HSD.

36. CHS 1 and CHS 2 also stated that Trinity Labs did not have equipment to conduct the CGx or Pharmacogenetic ("PGx")[2] tests on site and had to outsource the testing to PerkinElmer to conduct the CGx and PGx tests. In return, Trinity Labs paid PerkinElmer approximately $300 to $400 per CGx and PGx test, respectively. Once PerkinElmer completed the CGx and PGx tests, it returned the CGx and PGx tests' results back to Trinity Labs who then supposedly sent the results to the Medicare beneficiaries.

37. Bank records, obtained by grand jury subpoenas, demonstrate that Trinity Labs on or about November 2018 paid approximately $13,680 to PerkinElmer from a Wells Fargo Bank account ending 6339.

(ii) Medicare Claims Data

38. Between in or around April 2018 through in or around June 2019, Trinity Labs exclusively completed genetic screening tests and billed Medicare for approximately 134,392 genetic screening tests.

[2] PGx testing is a type of genetic test that assesses a patient's risk of an adverse response or likelihood to respond to a given drug, informing drug selection and dosing.

39. In comparison, from in or around November 2015 through in or around February 2018, Trinity Labs billed Medicare for approximately 36 genetic screening tests. From in or around April 2018 through in or around May 2019, Trinity Lab submitted approximately $89.2 million in claims to Medicare for genetic screening tests, of which Medicare paid approximately $35.3 million. The largest spike in billing occurred in or about January 2019 when Trinity Labs billed Medicare $15.8 million in one month.

(iii) Beneficiary Interviews

40. I, along with other law enforcement agents, interviewed several Medicare beneficiaries who received genetic screening test kits from Trinity Labs that were not medically necessary.

41. For example, on May 23, 2019, agents interviewed beneficiary R.M. In April 2019, R.M. explained that while attending a local senior health fair R.M. was approached by representatives of a company that had a booth set up for genetic screening tests. The representatives running the booth explained to R.M. that the test would be free of charge and covered by Medicare. The representatives informed R.M. that the test results would be sent directly to R.M.'s primary care physician ("PCP"), but instead the company sent the results to R.M.'s residence. R.M. took the result of the test to her PCP, who reviewed the result of the test and informed R.M. that the genetic screening tests results would not be useful to R.M. for at least another ten to twenty years. R.M. also noted that upon receiving and reviewing R.M.'s Explanation of Benefits ("EOB") from Medicare R.M. saw that approximately $20,000 was charged to Medicare for the genetic screening test by Trinity Labs.

42. Agents also interviewed beneficiary E.S., on June 7, 2019, who received two genetic screening test kits that contained paperwork and a cheek swab by mail. The kits were

preceded by a phone call from an unknown individual who inquired if E.S. completed and mailed the kits back to the sender. E.S. self-administered the one of tests and returned the test. E.S. completed the test because E.S. was under the impression, based on the phone call by the unknown individual, that the test could determine whether E.S. was genetically predisposed to cancer. E.S. also stated that E.S.'s PCP confirmed that E.S. did not have a medical necessity for the genetic test. E.S. provided agents with one of two original packages that contained the genetic screening test which showed that Company 1 was listed as a sender on the original package for the cheek swab packet sent to E.S. E.S. also received the results of the test *via* mail and provided agents with the original test result packet. Upon examination, agents noticed the packing slip for the test results listed the **Target Location**.

43. Also on June 7, 2019, beneficiaries R.S. and M.S., a married couple, were interviewed and they confirmed that they received genetic screening tests in the mail. They self-administered the swabs using instructions included in the kits and returned the swabs by mail using the postage-paid envelopes that came with the swab kits. M.S. explained that receipt of the genetic testing kits was preceded by a phone call with someone who explained that Medicare would cover the costs associated with the tests. M.S. also explained that the idea that the genetic test could tell them whether they had cancer came from either the person who called them or an advertisement for the genetic testing. Neither M.S. nor R.S. discussed the genetic test kits with their respective PCP. M.S. and R.S. received the tests results from Trinity Labs *via* U.S. mail.

44. On June 7, 2019, agents also interviewed beneficiary A.H. who verified receipt of a genetic screening test kit in the mail followed by multiple phone calls from an unknown individual asking confirmation of receipt of the genetic testing kit. A.H. agreed, after multiple calls, to complete the test because the caller convinced A.H. that that test was legitimate because,

among other reasons, the caller told A.H. that the results would be sent to A.H.'s PCP to help guide A.H.'s medical care and that the test would detect whether or not A.H. had cancer.

45. Agents also interviewed beneficiary C.B., on August 12, 2019, who stated that an unknown individual called in early 2019 and asked whether C.B. would be interested in completing a free genetic cancer screening tests. The caller told C.B. that the test was entirely covered by Medicare free of charge. Additionally, the caller asked about C.B.'s family health history and C.B. noted that C.B.'s uncles had been diagnosed with cancer. The caller then notified C.B. that C.B. would receive a genetic screening test kit in the mail, instructed C.B. to complete the test, and the results would be sent to C.B.'s PCP. When C.B. received the results they were negative for cancer, but C.B.'s PCP did not receive the results as promised by the caller.

(iv) Financial Analysis

46. A review and analysis of bank records, obtained through federal grand jury subpoenas, demonstrate that from 2018 through 2019 Trinity Labs sent approximately $25,187,639 through interstate wires from a Wells Fargo account ending in 6339 to companies owned by Berberian. Specifically, Trinity Labs sent the following interstate wires from the Wells Fargo account:

- approximately $17,837,639 to HSD;
- approximately $6,650,0000 to HSD Management LLC; and
- approximately $700,000 to HSD Financial LLC.

(v) Electronic Evidence

47. CHS 1 and CHS 2 provided law enforcement agents with access and consent to search their respective email accounts that they used to communicate with John Grisham, Lori

Grisham, and employees or representatives of Trinity Labs, and other individuals involved in the above-described genetic testing scheme.

48. Among the email accounts agents reviewed between CHS 1 and CHS 2 and John Grisham, Lori Grisham and employees or representatives of Trinity Labs the emails account addresses used the domain name "@trinityclinicallabs.com".

VI. PROBABLE CAUSE EXISTS TO BELIEVE EVIDENCE RELATING TO THE TARGET OFFENSES WILL BE FOUND AT THE TARGET LOCATION

49. Based on my training and experience, I know that it is common for laboratories like Trinity Labs, to store beneficiary claim files and other business documentation in electronic format on computer systems. Additionally, based on the CMS's rules and regulations and my training, I know that laboratories like Trinity Labs are required to maintain, and typically do maintain, beneficiary files for each beneficiary. These records are typically found at the business location for the laboratory.

50. Based on my training and experience, I also know that (a) fraud offenders keep records of their illegal activities for a lengthy period of time, even extending substantially beyond the time during which they actually produce, market, sell and profit from their crimes; (b) fraud offenders commonly maintain hard copy and computer files, books, records, receipts, notes, ledgers, journals, diaries, address books, and other sundry materials and papers relating to their crimes; (c) and such offenders often possess evidence, fruits, and instrumentalities relating to such offense in the places of business.

51. Based on my training and experience, and the evidence collected during the course of this investigation to date, I believe there is probable cause that Trinity Labs stores and keeps records including sham contracts between the HSD, Company 1 and Trinity Labs, patient medical

records and files, records containing financial data, and other information in hard copy and electronic form related to the **Target Offenses** at Trinity Labs' business office located at the **Target Location**, as described in Attachment A.

A. Trinity Labs' Registered Business Address is the Target Location

52. Texas Secretary State registration documents, signed by John Grisham, list Trinity Labs' business office at the **Target Location**.

B. Trinity Labs' Medicare Enrollment Form Requires Storage of Records at the Target Location

53. Additionally, Trinity Labs' Medicare enrollment application for Clinics Groups Practices/Group and Certain Other Suppliers (*i.e.*, CMS Form 855B) states that medical records are to be kept and stored at Trinity Labs' business address which is the **Target Location.** And I know that Medicare providers, such as Trinity Labs, are required to keep and store medical records for a period of seven years from the date of service.[3]

C. Beneficiaries received the CGx and PGx test results from Trinity Labs' Office located at Target Location

54. As noted above, beneficiary E.S. received two genetic testing kits that contained paperwork and a cheek swab by mail. E.S. received the results of the test and provided agents with the original packet E.S. received in the mail. The packing slip for the test results listed Trinity Lab with a business address located at the **Target Location**.

55. Moreover, beneficiaries R.S. and M.S. confirmed that they received a genetic testing kit from Trinity Labs *via* mail. The box that previously contained the kits was provided to agents and showed the packing slip in the packet listed the **Target Location**.

[3] *See* 42 C.F.R. § 424.516(f)(A).

D. Surveillance and Undercover Operation at Trinity Labs' at Target Location

56. On August 20, 2019, law enforcement agents conducted surveillance and completed an undercover operation at the **Target Location**. A law enforcement officer, in an undercover capacity (the "UCA"), entered Trinity Labs at the **Target Location**, with audio and video recording equipment to determine whether any activity occurred at the **Target Location** and whether Trinity Labs maintained computers and storage areas at the **Target Location**.

57. When the UCA approached the door entrance of the **Target Location** the UCA was met by a woman later identified as Lori Grisham. The UCA entered the interior of the **Target Location** while Lori Grisham held open the entrance door. While interacting with the UCA, Lori Grisham provided the UCA with a business card and stated that the name of the person on the business card, John Grisham, was her husband who operated Trinity Labs. Law enforcement officers later confirmed the identity of the woman who greeted the UCA as Lori Grisham by comparing her name and likeness to her driver's license photograph and public records that confirmed that she is married to John Grisham.

58. While interacting with Lori Grisham, from the entrance area, the UCA observed approximately 3 desk top computers, and an employee using 1 of the desk top computers at the **Target Location**. Additionally, at the **Target Location**, the UCA observed numerous lab specimens in carts and the paperwork associated with the specimens, various laboratory equipment, and approximately 3 employees, not including Lori Grisham.

59. Additionally, on September 11, 2019, while conducting physical surveillance from the parking lot area of the commercial building of the **Target Location**, I observed an individual park and exit a white Nissan Titan with a TX license plate number ending XXX2743 registered to John Grisham. I also saw the individual enter and exit the commercial building that houses the

Target Location. I then compared the driver's license photograph of the registered owner of the Nissan Titan and to the individual I saw in the parking lot of the **Target Location** and confirmed that it was John Grisham.

VII. MATERIALS SUBJECT TO SEARCH AND SEIZURE

A. Documents

60. Based on my training and experience, the records I am requesting to seize in Attachment B are kept in the normal course of business for laboratory companies such as Trinity Labs. These records include patient medical records and files, records containing financial data for John Grisham, Lori Grisham, or Trinity Labs and correspondence between John Grisham, Lori Grisham, CHS 1, CHS 2, representatives or employees of Company 1 and other known and unknown coconspirators that are likely to contain important information containing the execution of John and Lori Grisham's fraudulent activities.

B. Computers and Computer Equipment

61. In cases such as this, where health care claims are submitted electronically, computers, and computer equipment often contain evidence relating to the submission of those claims and other relevant business records.

62. Based on my knowledge, experience, and training, along with other law enforcement personnel with whom I have consulted on this issue, I know that the effective searches and seizure of evidence from computers commonly require law enforcement officers to seize most or all computer items (hardware, software and instructions) and then have these items processed later by a qualified computer forensic expert in a controlled laboratory environment (See Attachment B).

63. In addition, there is probable cause to believe that computers and their storage devices, monitors, keyboards, modems, printers, peripheral devices to scan or transmit data, as well as all internal and external storage devices are all instruments used in the commission of the **Target Offenses** and should be seized as such.

64. I submit that if a computer or storage medium is found at the Target Location,, there is probable cause to believe that records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, *i.e.*, in space of the storage medium that is not currently being used by an active file, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media – in particular, computers' internal hard drives – contain electronic evidence of how a computer has been used, what it has been used for, and who used it. To give a few examples,

this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

65. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the premises because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record

information about the dates files were created and the sequence in which they were created although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the **Target Offenses**, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally,

some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geo location information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored with a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely

reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

66. In most cases, a thorough search of a premise for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In *lieu* of removing storage media from the premises, it is sometimes possible to make an image copy of the storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination: As noted above, not all evidence take the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic

evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements: Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media: Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

67. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

VIII. RETENTION OF INFORMATION FOR AUTHENTICATION

68. In anticipation of litigation relating to the authenticity of data seized pursuant to the Warrant, the United States requests that it be allowed to retain a digital copy of all seized information authorized by the Warrant for as long as is necessary for authentication purposes.

IX. CONCLUSION

69. Based on my training and experience, and the facts as set forth in this affidavit, I believe that John Grisham, Lori Grisham, and Trinity Labs, along with other individuals and business entities, known and unknown, in this investigation committed and are continuing to carry out the **Target Offenses** and there are records of those **Target Offenses** as described in Attachment B and these records are presently located at the **Target Location**, as described in Attachment A. Accordingly, I respectfully request that a search warrant be issued for the **Target Location** located in the Eastern District of Texas.

JASON T. SETH
SPECIAL AGENT, HHS-OIG

Subscribed and sworn to before me this 25 day of September 2019.

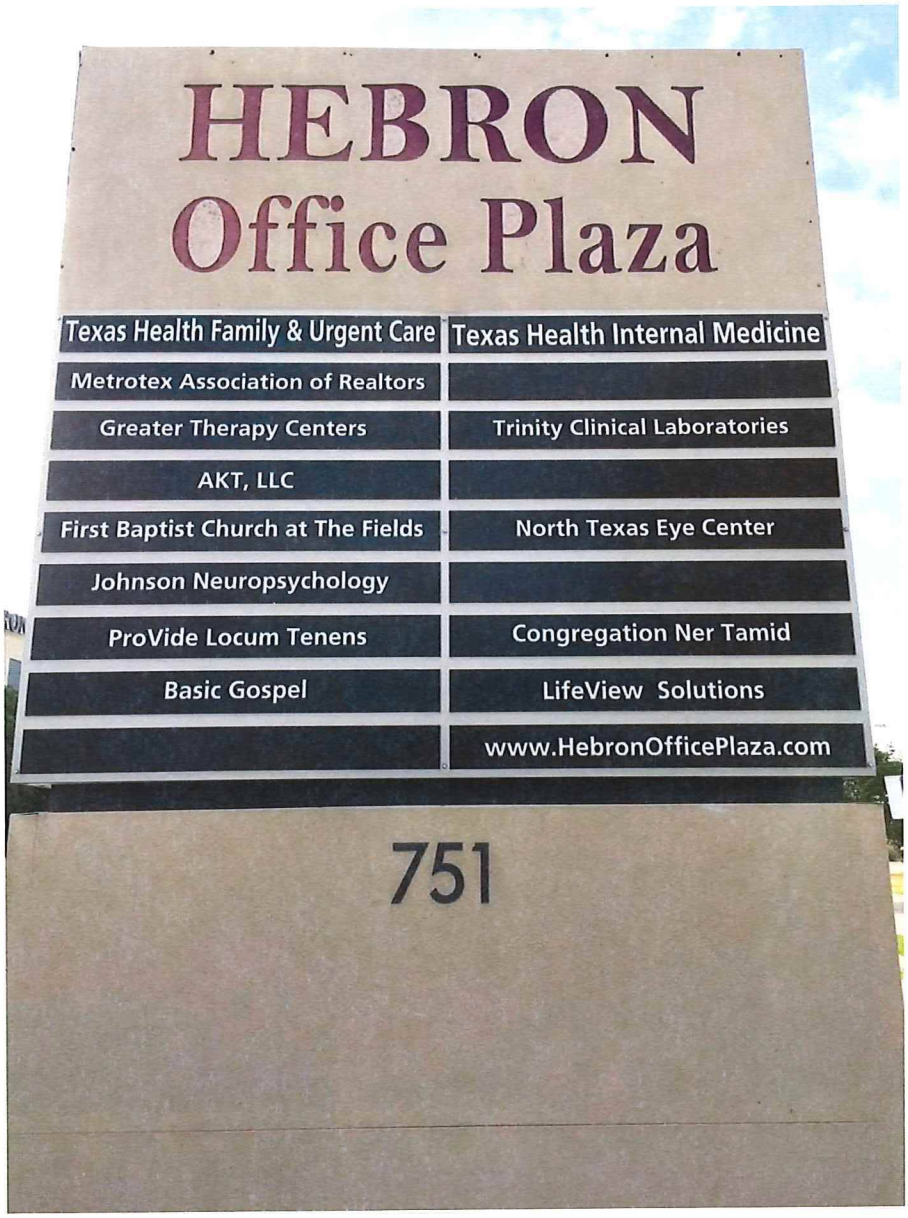
CHRISTINE A. NOWAK
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF TEXAS

ATTACHMENT A

PREMISES TO BE SEARCHED

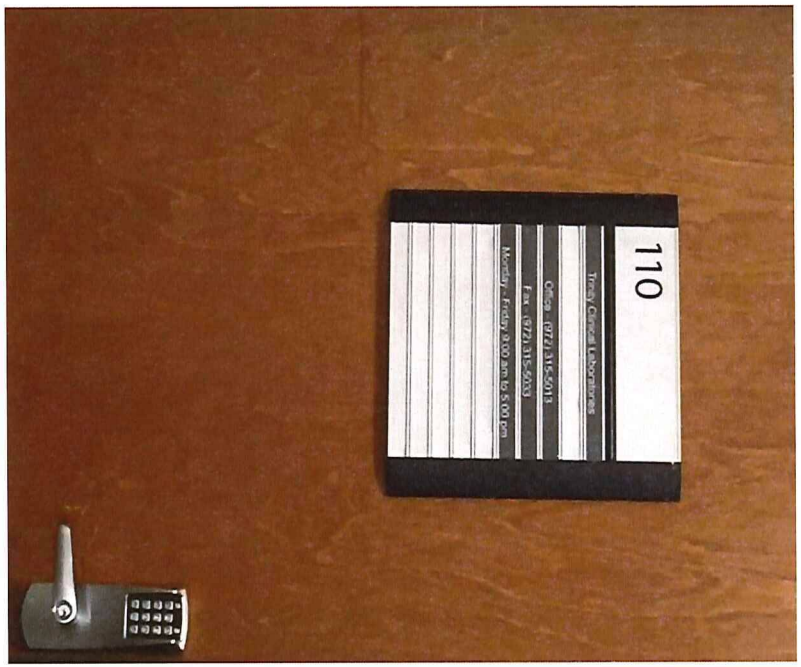
Property and premises to be searched:

Trinity Clinical Laboratories, LLC occupies an office suite in a multi-storied, commercial business building located at **751 Hebron Park Way, Suite 110, Lewisville, Texas, 75057**. The building is beige and cream and located close to the intersection of Hebron Park Way and Lakepointe Drive in Lewisville, Texas. There are multiple outdoor pylon signs, one located on Heron Parkway and another is located on Lakepointe Drive. One of the businesses listed on the outdoor pylon signs displayed in white lettering is "Trinity Clinical Laboratories". (See first photograph below). The exterior entry door for the building is located on the north side area of the building, has a beige metal awning, and is accessible from the sidewalk. A vehicle parking lot is directly in front of the entrance area. The front exterior doors are a double set tinted glass automatic sliding doors. The interior door for Trinity Labs is located on the first floor and is brown with black trim and a silver digital code lock handle on the right side of the door and a window to the right of the interior door, nearly the equivalent vertical length of the interior door. (See third photograph below). A sign is set over the front door entrance of the suite that states "110" in black print and business name "Trinity Clinical Laboratories, LLC". (See fourth photograph below).


HEBRON
Office Plaza
Texas Health Family & Urgent Care
Texas Health Internal Medicine
Metrotex Association of Realtors
Greater Therapy Centers
Trinity Clinical Laboratories
AKT, LLC
First Baptist Church at The Fields
North Texas Eye Center
Johnson Neuropsychology
ProVide Locum Tenens
Congregation Ner Tamid
Basic Gospel
LifeView Solutions
www.HebronOfficePlaza.com
751


NO PARKING


110


110
Trinity Clinical Laboratories
Office: (972) 315-5013
Fax: (972) 315-5033
Monday - Friday 8:00 am to 5:00 pm

ATTACHMENT B

PARTICULAR THINGS TO BE SEIZED FROM PREMISES

I. Particular Items and Information to be Seized by Law Enforcement

From in or about January 1, 2017, through the date this search warrant is executed, all records, documents, communications, data, and information located at Trinity Clinical Laboratories, LLC ("Trinity Labs") which occupies an office suite in a multi-storied, commercial business building located at **751 Hebron Park Way, Suite 110, Lewisville, Texas, 75057** (the "**Target Location**"), as described in Attachment A, involving John Grisham, Lori Grisham, or Trinity Labs, in whatever form that constitute evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 371 (Conspiracy to Defraud the United States and to Pay and Receive Health Care Kickbacks), 42 U.S.C. § 1320a-7b (Anti-Kickback Statute), 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1349 (Conspiracy to Commit Health Care Fraud), and 18 U.S.C.§ 1347 (Health Care Fraud) including:

1. All correspondence, including memos, letters, and emails concerning the medical necessity and/or delivery of services billed to a federal health care benefit program, including but not limited to payments for referrals to patient referral sources, face sheets, referral tracking logs, patient census logs, and correspondence with any physicians, non-physician practitioners, or telemedicine companies.

2. Patient billing records, itemized billing records, Explanation of Benefit forms, letters to patients explaining their bills, letters from patients inquiring about their bills, and any documents or memoranda concerning patient billings.

3. All documents relating to the filing for, receipt of, billing of, and deposit of insurance claims, including but not limited to Medicare claims, Medicaid claims and private-pay

insurance program claims, patient lists, supporting documentation, notes, invoices, and records of insurance payments received.

4. All documents concerning the computer billing system, or any other methods of posting charges manually or otherwise, preparing invoices, making adjustments or alterations in billing, generating billing reports, or other procedural operations associated with the tracking of services rendered and billing, including accounts receivable journals and ledgers.

5. All personnel files of employees or contractors, including social workers, staff assistants, professional counselors, coding/billing staff, and administrative staff to include such documents as applications for employment, employment contracts, employee and contactor work schedules, salaries and compensation, bonuses, time sheets, reference/background checks, professional certifications, training, performance evaluations, disciplinary actions, improvement plans, and payroll records for all employees and contractors.

6. All records regarding the formation and operation of companies, corporations and/or LLCs.

7. All address and/or telephone books and papers reflecting names, addresses, telephone numbers, email addresses, or website addresses, of financial institutions and other individuals or businesses with whom a financial relationship exists.

8. All insurance training manuals, provider manuals, regulations, bulletins, reports, newsletters, notices, pamphlets, and correspondence related to proper billing and documentation procedures and any documentation regarding instructions for billing insurance providers/carriers, including but not limited to: Medicare, Medicaid and private-pay insurance programs.

9. All office policies and procedures related to treatment records documentation, insurance billing, and patient referrals.

10. All corporate, business, and personal tax returns, including any quarterly employment tax returns, federal income tax returns, state tax returns, IRS Form 1099(s), and any records/correspondence to or from tax advisors or tax return preparers.

11. Any non-privileged documents related to any administrative action involving John Grisham, Lori Grisham, or Trinity Labs including any settlement-related documents.

12. All correspondence with insurance providers requesting supporting documentation, or alerts regarding billing and coding practices, including information related to any private and government insurance audits, audit findings and/or results as well as any documents related to overpayments recoveries.

13. All financial documents identifying any accounts under the control of John Grisham, Lori Grisham, or Trinity Labs, including but not limited to books of account, records of asset acquisition, banking transactions, bank statements, bank ledgers, bank deposit slips, Certificate of Deposit statements, safety deposit box records, investment and retirement account statements, records of the discharge of debt, loans, notes payable, records of expenses, stocks, bonds or other financial instruments set up by or under the control of John Grisham, Lori Grisham, or Trinity Labs.

14. All documents identifying any businesses or corporations which John Grisham, Lori Grisham, or Trinity Labs, has a financial relationship with, investment stake in or controlling interest of, including, but not limited to, contracts, articles of incorporations, shareholder agreement, or memorandum of understanding.

15. All documents and records for John Grisham, Lori Grisham, or Trinity Labs , including but not limited to patient records and/or patient files, physician notes, technician notes, radiographs and images, all office visit notes, calendars, appointment books, patient sign-in sheets,

prescriptions and prescription pads, insurance records, billing or payment information receipts, receipt books, ledgers documenting payments made or received, and any cash register or credit card reader printouts or receipts.

16. All documents, contracts or agreements between John Grisham, Lori Grisham, or Trinity Labs and any third party, including, but not limited to independent contractor agreements.

17. All computers or storage media capable of being used to commit the offenses, further the activity, or store evidence, including computer-generated or stored documents reflecting patient information, medical and/ or mental health records, billing or payment information, financial records, medical and/or psychological tests and results, appointments, or insurance records of the patients.

18. All documents relating to any marketing, public relations, or other promotions.

19. Any assets evidencing the disposition of illegal proceeds generated from criminal activities, including but not limited to, monetary instruments including currency, cashier's checks, money orders, traveler's checks, precious metal, and any other negotiable bearer instruments.

20. All calendars, date books, employee schedules, employee sign-in sheets, and travel records.

21. All correspondence, including memoranda, letters, and emails.

22. All documents reflecting John Grisham's, Lori Grisham's, or Trinity Labs' revenue and sources of income, including without limitation applications for credit, financing, or loans of any kind.

23. Records of control over other areas such as storage units where financial, medical and other billing records may be maintained.

24. Records evidencing control of the business or premises of the **Target Location**, namely utility bills, telephone bills, rent or lease records pertaining to or evidencing ownership or control of the premises to be searched.

25. Any computer, computer hard drive, electronic device, or other physical object upon which computer data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain items to be seized otherwise called for by this warrant:

a. Evidence of who used, owned, or controlled the COMPUTER at the time the items to be seized described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. Evidence of the lack of such malicious software;

d. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. Evidence of the times the COMPUTER was used;

g. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. Records of or information about Internet Protocol addresses used by the COMPUTER;

j. Records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

k. Contextual information to understand the evidence described in this attachment.

26. As used above, the terms, "documents," "records," and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

27. The term "COMPUTER" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing electronic devices performing logical, arithmetic, or storage functions for electronically stored information, including desktop computers, notebook computers, cell phones, mobile devices such as smart phones and tablets, server computers, virtual computer systems, and network hardware.

28. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include computer disks, data disks, hard disks, RAM, floppy disks, flash memory, CD-ROM disks, mobile devices, smart phones, tablets, and other magnetic and/or optical media.

30. Any container, file box, filing cabinet, storage unit, or other storage facility which exclusively or virtually exclusively contains items to be seized or other items authorized to be seized pursuant to this warrant, which are a means of committing a violation of 18 U.S.C. § 371 (Conspiracy to Defraud the United States and to Pay and Receive Health Care Kickbacks), 42 U.S.C. § 1320a-7b (Anti-Kickback Statute), 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1349 (Conspiracy to Commit Health Care Fraud), and 18 U.S.C.§ 1347 (Health Care Fraud), and subject to seizure pursuant to rule 41 of the Federal Rules of Criminal Procedure.

II. Review of Evidence Seized by Law Enforcement

With respect to law enforcement's review of the items seized at the **Target Location**, as described in Attachment B, law enforcement (*i.e.*, the federal agents and prosecutors working on this investigation and prosecution), along with other government officials and contractors whom law enforcement deems necessary to assist in the review of the items seized at the **Target Location** (collectively, the "Review Team") are hereby authorized to review, in the first instance, items seized at the **Target Location** and the information and materials contained in them, as set forth in this Attachment B.

If law enforcement determines that all, some, or a portion of the information or materials in the items seized at the **Target Location** contain or may contain information or material subject to a claim of attorney-client privilege or work-product protection (the "Potentially Privileged

Materials"), the Review Team is hereby ordered to: (1) immediately cease its review of the specific Potentially Privileged Materials at issue; (2) segregate the specific Potentially Privileged Materials at issue; and (3) take appropriate steps to safeguard the specific Potentially Privileged Materials at issue.

Nothing in this Attachment B shall be construed to require law enforcement to cease or suspend the Review Team's review of the items seized at the **Target Location** upon discovery of the existence of Potentially Privileged Materials in one or more of the items seized at the **Target Location**.